< KTRL+INFORME >

Análisis del formulario “Medellín me cuida”

Alcaldía de Medellín

www.medellin.gov.co/medellinmecuida

Este informe se basa en investigaciones que se hicieron principalmente entre 11 y el 14 de abril 2020.

Antes de hacer los análisis que implicaran llenar formularios, se envió un correo electrónico a “webmaster@medellin.gov.co” y también se envió el mismo mensaje a través del formulario PQRS del sitio (registro de solicitud n° 1139371325060066995).

Introducción y descripción de la metodología

El presente documento presenta los resultados del análisis que hizo el laboratorio de seguridad digital y privacidad de la Funfación Karisma (K+Lab) del formulario web “***Medellín me cuida***”[1] construido “*en el marco de la emergencia sanitaria ocasionada por el COVID-19*” . Este formulario esta albergado en el sitio de la Alcaldía de Medellín quien esta responsable del tratamiento de datos asociados. Nuestro análisis se enfocó en transparenica e información, privacidad y seguridad digital. Los resultados se presentan de forma sintética en una tabla completada con elementos técnicos que aparecen en anexo.

Este análisis puso a la luz una vulnerabilidad de seguridad digital importante, que primero se sociabilizó con la Alcaldía de Medellín para que se resolviera, previamente a toda publicación.

Se encontraron también vulnerabilidades de impacto más leves que al día de esta publicación no se han resuelto todavía y por lo tanto se quitaron las partes de este informe en su versión pública. El objetivo de este trabajo siendo de contribuir al mejoramiento de la seguridad digital y no de facilitar un ataque.

La metodología que usamos se basa análisis técnicos externos y no intrusivos. Se analizaron la información pública, el código fuente de la página web (HTML/javascript), las cookies y los flujos de datos/paquetes generados alcompletar el formulario. Para esto, se usaron las herramientas de código abierto siguientes:

- navegadores *Mozilla/Firefox*, *Waterfox*[2] y *Chromium* ;
- la extensión de navegador *Cookie Manager +*[3] ;
- la herramienta de captura de flujos/paquetes HTTP(S) (proxy) *OWASP ZAP*[4].

Los análisis se hicieron después de avisar la Alcaldía de Medellín [ver Anexo 0].

Se mencionan en italico cuando se ha realizado una mejora entre el día del análisis y el de la publicación de este informe.

1 “Medellín me cuida”, www.medellin.gov.co/medellinmecuida

2 Waterfox (https://www.waterfox.net/) es un navegador derivado de Mozilla/Firefox, de código abierto (Mozilla Public License, version 2.0). Permite un alto nivel de configuración y de compatibilidad con las extensiones

3 https://github.com/vanowm/FirefoxCookiesManagerPlus

4 https://www.zaproxy.org/
Hay que mencionar que esta herramienta se usó exclusivamente en “modo seguro” de tal manera que se hicieran sólo análisis no intrusivos, del lado del cliente de nuestro computador), analizando los flujos de datos saliendo y entrando de nuestro navegador.

Tabla sintética del análisis del formulario

“Medellín me cuida”

Política de datos ***Se ha creado unos términos y condiciones del uso de la plataforma “Medellín me cuida” al día de la publicación de este informe***	Existen dos documentos (link al final del formulario) generales: • la “*POLÍTICA DE PRIVACIDAD Y CONDICIONES DE USO DEL SITIO WEB OFICIAL DE LA ALCALDÍA DE MEDELLÍN WWW.MEDELLIN.GOV.CO*”; • el Decreto 1096 de 2016 por medio del cual se deroga al dercreto 01693 del 2015 y se adopta la política para el tratamiento de datos personales en el municipio de Medellín. **En el primer documento hay un numeral** para los tratamientos vinculados con el formulario “Medellín me cuida” (www.medellin.gov.co/medellinmecuida) pero es muy general. Sólo apunta a que el tratamiento de datos personales se hará “*en el marco de la emergencia sanitaria ocasionada por el COVID-19*” sin más precisiones sobre las finalidades. Además se refiere al decreto (política de tratamiento de datos) que da a la alcaldía posibilidades de transferencias de datos muy amplias hacia otros entidades [ver Anexo 1].
Datos colectados (en el formulario “*Medellin me cuida*”)	Se piden los datos personales y de salud siguientes: • tipo y número de documento; • nombre y apellido; • n.º de contrato EPM; • dirección; • teléfono celular (obligatorio) y fijo (facultativo); • profesión (facultativo); • edad; • correo electrónico; • enfermedades crónicas y prácticas que favorecen la enfermedad (hipertensión, cancer, diábetes, obesidad, fumador, etc.); • síntomas (tos, fiebre, dificultad para respirar, etc.). El formularios permite **añadir familiares** y llenar el cuestionario para ellos también.
Alojamiento del servidor	El servidor web (@IP: 200.13.232.188) está alojado **en Colombia** en la empresa ***EPM Telecomunicaciones***.
Certificado SSL/TLS y HTTPS	Sí, la página usa el protocolo **HTTPS**, con un certificado Digicert “Extended Validation”, con una muy buena nota (“A”) en la evaluación de SSLLABS. Sin embargo, **hay un problema leve de configuración del certificado,** que es valido sólo para “www.medellin.gov.co”**.** Esto hace que si uno entra en la página de inicio sólo con “medellin.gov.co” (sin el “www”) el navegador levanta una alerta de seguridad. No es grave en absoluto pero puede dar una mala imagen del sitio web de la Alcaldía de Medellín. Se podría probablemente resolver fácilmente cambiando las propriedades del certificado con DigiCert o con la configuración del DNS. [Anexo 2]

Envió de datos del formularios	Los datos del formulario se envían de manera segura con el protocolo HTTPS (método POST) hacia la url “medellin.gov.co/medellinmecuida”. La solicitud incluye una cookie de autenticación de sesión (“cookiesesion1” protegida con “Http Only”), una cookie de sesión Java (JSESIONID) y una cookiexz del sistema SAP. [Anexo 3]
Interconexión con el servidor de EPM : una vulnerabilidad grave ***Se ha resuelto esta vulnerabilidad al día de la publicación de este informe***	El análisis de flujos de datos recibidos por nuestro computador al entrar los datos en el formulario muestra una **vulnerabilidad importante vinculada con la consulta de contratos EPM**. Al entrar el número de contrato EPM solicitado en el formulario, se generan solicitudes a un servidor externo de EPM (dominio “epm.adminfo.net”, @IP:190.248.11.235 que pertenece a EPM). Esta solicitud se genera tras la ejecución de una función javascript alojada en el servidor de la alcaldía. **El servidor de EPM responde con datos personales detallados de la persona titular del contrato** (nombre, apellido, dirección, coordenadas GPS, estrato, riesgo, valor de factura) de los cuales sólo la dirección se autocompleta de manera visible en el formulario. **Esto requiere solo el número de contrato, que parece secuencial, sin necesitar autenticación**. El [Anexo 4] muestra esta vulnerabilidad desde un punto de vista técnico. Hay que precisar que llenamos el formulario con el número de contrato propuesto en el ejemplo del formulario (“44951”, que aunque parecía ficticio, parece ser un número de contrato real). Pensamos que la vulnerabilidad es grave y que usando la URL que aparece en nuestra captura, se podría acceder a los datos de otros clientes e incluso quizás automatizar el proceso para sacar información personal de la base de datos de EPM. Hay que resaltar que la vulnerabilidad se origina desde el servidor de EPM pero este formulario web crea la interconexión con el, y hace de cierta forma la vulnerabilidad más visible. [Ver Anexo 4]
Rastreadores y cookies de terceros	No hay en la página del formulario. Pero varios rastreadores publicitarios en la página principal (de inicio). El único servicio externo que se usa el Google “Re Capcha”.
Versión del servidor web y actualizaciones	[se quito esta parte del informe en esta versión pública] Bajo ciertas condiciones, esta versión podría tener una vulnerabilidad (de impacto moderado, y poco detallada públicamente).
Otros puntos de seguridad para mejorar	Algunos problemas (moderados) fueron detectados con análisis semi-automático y manuales de las respuestas del servidor web (análisis de flujos). Las principales son: [se quitó esta parte del informe en su versión pública]

ANEXOS – Referencias

[0] Correo preliminar enviado a los encargados el sitio

Asunto:Análisis de formularios del sitio web de la Alcaldía de Medellín
Fecha:*Sun, 12 Apr 2020 16:03:20 -0500*
De:*XXX@karisma.org.co*
Organización:*Fundación Karisma*
Para:*webmaster@medellin.gov.co*
CC:*XXX*

La Fundación Karisma es una organización de la sociedad civil, fundada en 2003 y localizada en Bogotá, que busca responder a las oportunidades y amenazas que surgen en el contexto de la “tecnología para el desarrollo” para el ejercicio de los derechos humanos. Karisma trabaja desde el activismo con múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.
Desde hace varios años estamos evaluando aspectos de seguridad y privacidad de algunas páginas web y aplicaciones asociadas con trámites y servicios de interés público. Recientemente lo hicimos con la aplicación del Instituto Nacional de Salud "CoronApp". Estos análisis han sido de conocimiento del Ministerio de Tecnologías (MINTIC) que en varias ocasiones nos ha facilitado mecanismos de comunicación con los responsables de las plataformas evaluadas. Los análisis han llevado a mejoras de las plataformas. Esperamos que este sea nuevamente el caso.
En este momento estamos haciendo un análisis no intrusivo de los formularios del sitio web de la Alcaldía de Medellín vinculados con la gestión de la epidemia actual, en especial con Medellín me cuida, en estos aspectos de privacidad y seguridad digital. Parte de nuestra evaluación incluye el análisis del tráfico de datos generado por los formularios que recopilan información personal, y por esto, queremos comunicarles que encontrarán registros a nombre de Karisma, asociados al correo test@karisma.org.co. Estos datos no son reales y no deben ser tomados en cuenta para los reportes de salud ni la generación de alertas.
Una vez tengamos el informe de nuestros hallazgos los daremos a conocer en primera instancia a ustedes.
Si tienen alguna duda o inquietud sobre el tema pueden comunicarse con nosotros respondiendo este correo. Estaremos atentos a contestar cualquier pregunta.

Atentamente,

Fundación Karisma.

Además, se envió el mismo mensaje a través del formulario PQRS del sitio (registro de solicitud n° 1139371325060066995).

[1] Extractos de la política de privacidad del Decreto 1096

"*POLÍTICA DE PRIVACIDAD Y CONDICIONES DE USO DEL SITIO WEB OFICIAL DE LA ALCALDÍA DE MEDELLÍN WWW.MEDELLIN.GOV.CO*", Numeral 8:

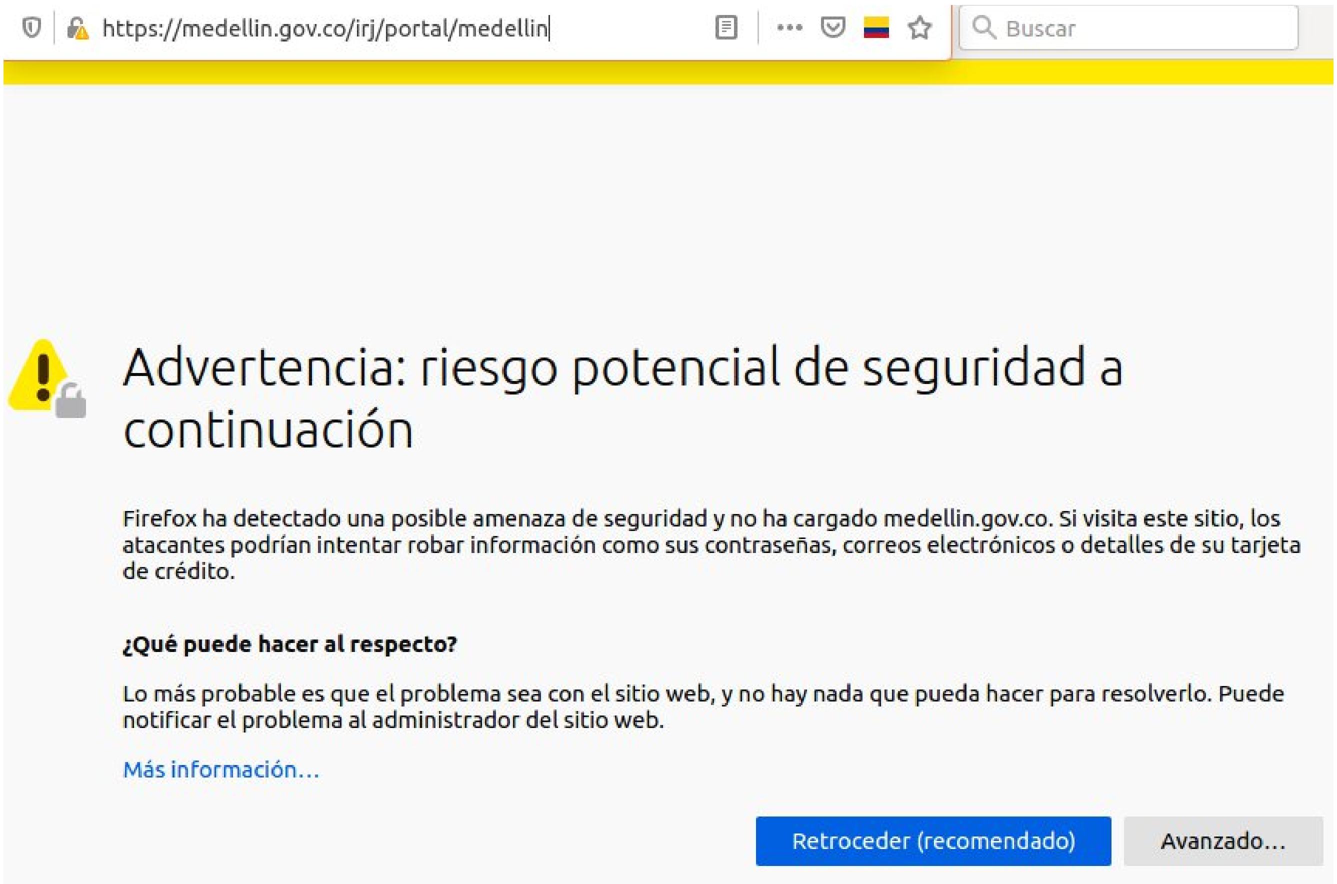
> *8. PRECISIÓN ESPECIAL FRENTE AL FORMULARIO "MEDELLIN TE CUIDA"*
> *De conformidad con lo definido por la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013, el Decreto Municipal 1096 de 2018 y demás normas concordantes a través de las cuales se establecen disposiciones generales en materia de hábeas data y se regula el tratamiento de la información que contenga datos personales. Declaro que autorizo al Municipio de Medellín para la recolección y tratamiento de mis datos personales, entiendo que los datos serán objeto de recolección, almacenamiento, uso, circulación, supresión, transferencia, transmisión, cesión y todo el tratamiento necesario, en el marco de la emergencia sanitaria ocasionada por el COVID -19.*

Decreto 1096 de 2016 por medio del cual se deroga al dercreto 01693 del 2015 y se adopta la política para el tratamiento de datos personales en el municipio de Medellín, numeral XIII.

XIII. DIVULGACIÓN DE INFORMACIÓN A TERCEROS: El Municipio de Medellín puede compartir información personal de sus servidores, empleados, contratistas, proveedores, usuarios, ciudadanos y demás Titulares, con cualquier tercero que, en virtud de una relación contractual o legal que éste tenga con el Municipio de Medellín, requiera tener acceso a dichos datos personales.	Adicionalmente, se podrán compartir los datos personales recolectados con terceros aliados o contratistas del Municipio de Medellín, así como con otras entidades del orden municipal, departamental y nacional, con el objeto de que le presten servicios a éste o en nombre de éste, o para la ejecución de planes, programas, proyectos o estrategias conjuntas o, en general, cuando tal acceso o transferencia se requiera por disposición legal.

[2] Problema de implementación del certificado SSL/TLS

Cuando se entra directamente la dirección del sitio web de la Alcaldía en el navegador "medellin.gov.co", el mensaje de alerta siguiente aparece:



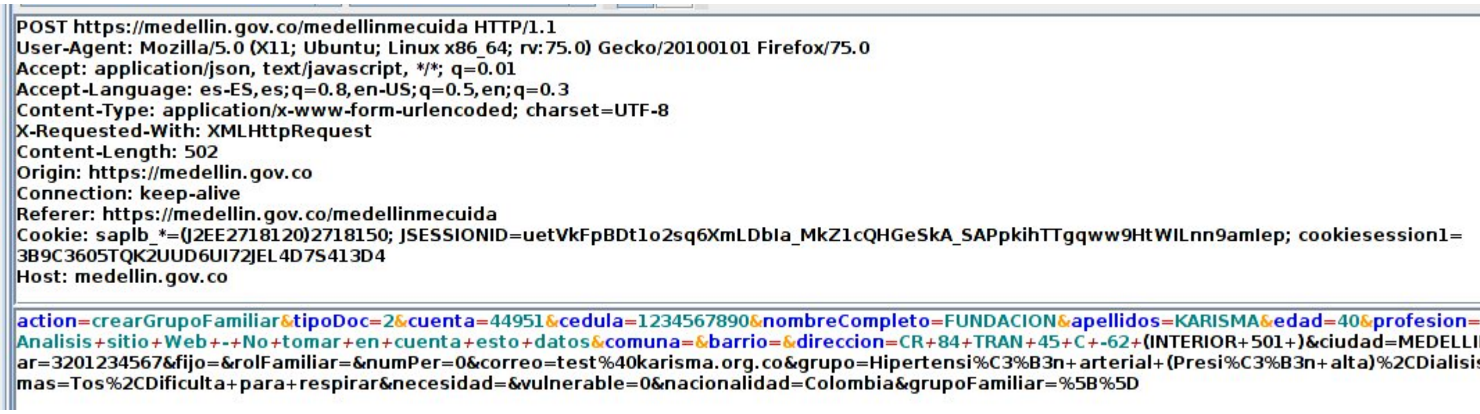
Esta alerta no aparece cuando uno entra con la dirección, incluyendo el "www". En este caso la conexión aparece como "conexión segura":



Esto no es grave en absoluto pero da una mala imagen del sitio y se podría resolver fácilmente cambiando los parámetros del certificado (extendiendo su validez a todo el dominio "medellin.gov.co") o creando un alias (CNAME) de "medellin.gov.co" hacia "www.medellin.gov.co" en el servidor DNS.

[3] Envió de Datos a través del formulario

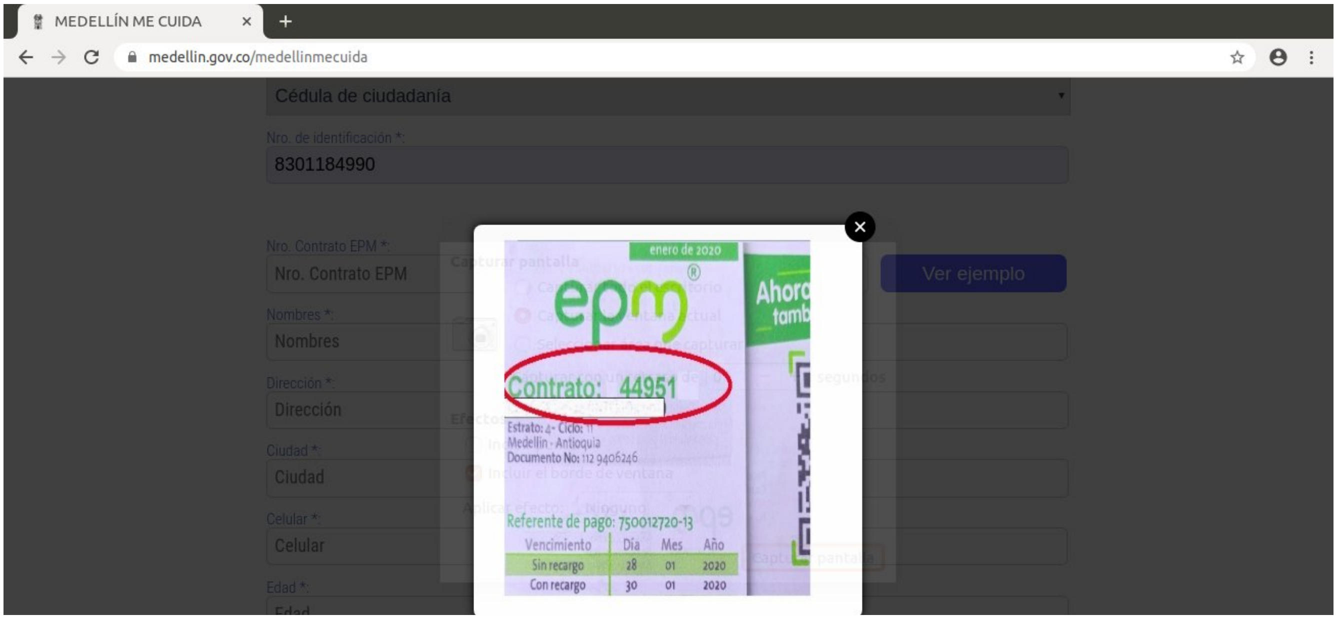
Así se ve el envió de datos – a través de la herramienta de código abierto OWASP ZAP[51] – que usamos:



```
POST https://medellin.gov.co/medellinmecuida HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 502
Origin: https://medellin.gov.co
Connection: keep-alive
Referer: https://medellin.gov.co/medellinmecuida
Cookie: saplb_*=(J2EE2718120)2718150; JSESSIONID=uetVkFpBDt1o2sq6XmLDbla_MkZ1cQHGeSkA_SAPpkihTTgqww9HtWILnn9amlep; cookiesession1=
3B9C3605TQK2UUD6UI72JEL4D7S413D4
Host: medellin.gov.co

action=crearGrupoFamiliar&tipoDoc=2&cuenta=44951&cedula=1234567890&nombreCompleto=FUNDACION&apellidos=KARISMA&edad=40&profesion=
Analisis+sitio+Web+-+No+tomar+en+cuenta+esto+datos&comuna=&barrio=&direccion=CR+84+TRAN+45+C+-62+(INTERIOR+501+)&ciudad=MEDELLI
ar=3201234567&fijo=&rolFamiliar=&numPer=0&correo=test%40karisma.org.co&grupo=Hipertensi%C3%B3n+arterial+(Presi%C3%B3n+alta)%2CDialisis
mas=Tos%2CDificulta+para+respirar&necesidad=&vulnerable=0&nacionalidad=Colombia&grupoFamiliar=%5B%5D
```

Se nota que el envió se hace con el protocolo HTTPS y el método POST. Se usaron datos de Karisma mencionando “Análisis sitio Web – No tomar en cuenta” en la parte profesión. Se usó el número de contrato EPM propuesto como ejemplo en el sitio web (44951, haciendo clic en “ver ejemplo”):



5https://www.zaproxy.org/

Hay que mencionar de nuevo que esta herramienta se usó exclusivamente en “modo seguro” de tal manera que se hicieran sólo análisis no intrusivos, del lado del cliente de nuestro computador), analizando los flujos de datos saliendo y entrando de nuestro navegador.

[4] Vulnerabilidad en la interconexión con el servidor EPM

El análisis de flujo mostró la solicitud HTTPS y su respuesta siguiente:

```
GET https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id=44951&_=1586810468367 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Origin: https://medellin.gov.co
Connection: keep-alive
Referer: https://medellin.gov.co/medellinmecuida
Host: epm.adminfo.net
```

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 20:42:33 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1;mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=631138519
X-Permitted-Cross-Domain-Policies: none
Content-Length: 413
Connection: close
Content-Type: application/json; charset=UTF-8
```

[**Aquí se recortó el contenido de la respuesta del servidor porque dejaba aparecer muchos datos personales del cliente: nombre, apellido, dirección, coordenadas GPS, estrato, nivel de riesgo, valor factura**]

En la respuesta del servidor web, se puede observar datos personales detallados del cliente (incluso el resultado de una evaluación de riesgos interna a la empresa), sin que se hubiera necesitado ninguna autenticación o información adicional. En el formulario web, de todos estos datos, sólo aparece la dirección correspondiente, que se autocompleta.

Esta solicitud se hizo automáticamente al entrar el número de contrato EPM dado cómo ejemplo en el formulario (ver Anexo 3). Técnicamente, se originó después de la ejecución de una función javascript llamada "familiaExt.js", alojada en el servidor web de "medellin.gov.co". Así aparece en nuestra captura de flujo, junto con la respuesta del servidor que responde con el código javascript de la función donde aparece la solicitud hacia el dominio "epm.admininfo.net":

Método	URL
GET	https://medellin.gov.co/epfcovi2/scripts/familia/familiaExt.js?sid=0.8650184815370987
GET	https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id=44951&_=1586810468365
GET	https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id=44951&_=1586810468365

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 20:41:08 GMT
Server: SAP NetWeaver Application Server 7.22 / AS Java 7.31
content-type: application/x-javascript
last-modified: Mon, 13 Apr 2020 20:34:07 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/epfcovi2
content-length: 43494
Via: 1.1 www.medellin.gov.co
Vary: Accept-Encoding
Keep-Alive: timeout=12
Connection: Keep-Alive
```

```
}

function validarNumEPM(datos){
	var path = window.location.pathname;
	var path = 'https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id='+datos.trim();
//	var data = $.param({
//		action			: 'consultarPorNumeroContrato',
//		cuenta			: datos
//	});

	setLoading(true);
	$.ajax({
		url	: path,
```

Esto significa que si bien la vulnerabilidad no es propiamente del servidor web de la Alcaldía sino de un servidor de EPM, la conexión hacia este servidor se origina por la ejecución de una función Javascript alojada en el servidor de la Alcaldía.

El problema no sólo es grave porque se devuelven datos del cliente que no deberían y ni siquiera son útiles pero también porque pensamos que haciendo variar el id de contrato en la URL solicitada se podría acceder a los datos de otros clientes.

https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?**id=XX**&_=1586810468365

Quizás además el proceso se pueda automatizar con un script que pudiera sacar toda o parte de la base de datos de clientes de EPM.